Anomaly Detection Report

Model: autoencoder

Source File: orglog1.csv

Total Anomalies Found: 11

Anomaly #0 (Score/Error: 0.0635)

```
Request: GET /utxLogin/login HTTP/1.1
Status: 302 | Bytes: 249 | IP: 0.0.0.0
```

Reason: Classified as anomaly due to high reconstruction error in 'Size'.

Anomaly #1 (Score/Error: 0.0613)

```
Request: GET / HTTP/1.1
Status: 302 | Bytes: - | IP: 0.0.0.0
```

Reason: Classified as anomaly due to high reconstruction error in 'Duration'.

CRITICAL Anomaly #2 (Score/Error: 0.0979)

```
Request: GET / HTTP/1.1
Status: 302 | Bytes: - | IP: 0.0.0.0
```

Reason: This anomaly is likely indicative of a possible Path Traversal attack as the unusually low duration, size, and presence of a POST method in the request on a root directory could suggest an attempt to access unauthorized directories or files on the server.

CRITICAL Anomaly #3 (Score/Error: 0.0979)

```
Request: GET / HTTP/1.1
Status: 302 | Bytes: - | IP: 0.0.0.0
```

Reason: Possible Path Traversal attack: A GET request with a small duration and size, along with the presence of a POST method in the anomaly features, suggests an attempt to access unauthorized directories or files on the server through manipulating the HTTP request methods.

Anomaly #4 (Score/Error: 0.0613)

```
Request: GET /utxHomeApp/redirectToHome HTTP/1.1
Status: 302 | Bytes: - | IP: 0.0.0.0
```

Reason: Classified as anomaly due to high reconstruction error in 'Duration'.

CRITICAL Anomaly #5 (Score/Error: 0.0979)

```
Request: GET / HTTP/1.1
Status: 302 | Bytes: - | IP: 0.0.0.0
```

Reason: Likely Brute Force Attack: The anomaly in the server log with a short duration, small size, and POST method usage suggests a potential brute force attack attempting to guess login credentials.

Anomaly #6 (Score/Error: 0.0613)

Anomaly Detection Report

Request: GET /boardwebapp/company/ HTTP/1.1
Status: 302 | Bytes: - | IP: 0.0.0.0

Reason: Classified as anomaly due to high reconstruction error in 'Duration'.

Anomaly #7 (Score/Error: 0.0613)

Request: GET /utxHomeApp/redirectToHome HTTP/1.1
Status: 302 | Bytes: - | IP: 0.0.0.0

Reason: Classified as anomaly due to high reconstruction error in 'Duration'.

Anomaly #8 (Score/Error: 0.0158)

Request: GET /agmipad/ HTTP/1.1
Status: 302 | Bytes: - | IP: 0.0.0.0

Reason: Classified as anomaly due to high reconstruction error in 'Status'.

Anomaly #9 (Score/Error: 0.0021)

Request: GET /pAccounting/appResources/js/angular/controller/fcm/fcmSupportController.js?v=/../../../../../../../../bin/id%00| HTTP/1.1
Status: 200 | Bytes: 2202 | IP: 0.0.0.0

Reason: Classified as anomaly due to high reconstruction error in 'Duration'.

Anomaly #10 (Score/Error: 0.0006)

Request: GET /pAccounting/extResources/tooltip/tipsy-docs.js?v=/..//..///../..//../..//../..//../..//../..///../..///etc/passwd%00 HTTP/1.1
Status: 200 | Bytes: 931 | IP: 0.0.0.0

Reason: Classified as anomaly due to high reconstruction error in 'Duration'.
